CLAIMS

What is claimed, is:

1. A data storage device for an information processing device, the data storage device comprising:

an encryption circuit for encrypting desired data and personal identification information by use of an encryption key created out of a given piece of the personal identification information;

a recording medium for recording the data and the personal identification information encrypted by the encryption circuit; and

a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium.

2. The data storage device according to claim 1,

wherein the encryption circuit encrypts the encryption key by use of a different encryption key, and

the recording medium records the encryption key encrypted by use of the different encryption key.

3. The data storage device according to claim 1,

wherein the recording medium includes a special storage area which is inaccessible in normal use, and

the recording medium records the encryption key in the special storage area.

4. The data storage device according to claim 1,

wherein the encryption circuit creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and

the recording medium manages the storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys.

5. A data storage device for an information processing device, the data storage device comprising:

an encryption circuit for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key created out of a given piece of the personal identification information;

a recording medium for recording the data encrypted by use of the first encryption key, the first encryption key encrypted by use of the second encryption key, and the personal identification information encrypted by use of the second key; and

a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium.

6. The data storage device according to claim 5,

wherein the encryption circuit decrypts the encrypted first encryption key being read out of the recording medium by use of the second encryption key, and executes any of encryption and decryption of the desired data by use of the

decrypted first encryption key.

7. A hard disk device comprising:

a magnetic disk being a recording medium;

a read-and-write mechanism for writing and reading data in and out of the magnetic disk; and

a control mechanism having an encryption function for encrypting data to be written in the magnetic disk and for decrypting the encrypted data to be read out of the magnetic disk, the control mechanism for controlling reading and writing the data by the reading-and-writing mechanism,

wherein the control mechanism executes encryption of the data to be written in the magnetic disk for each unit of writing and reading data in and out of a storage area of the magnetic disk upon processing of writing the data in the magnetic disk, in response to turning on and off of the encryption mechanism.

8. The hard disk device according to claim 7,

wherein the control mechanism judges as to whether the data are encrypted or not upon reading the data out of the storage medium, and further decrypts the data when the data are encrypted.

9. The hard disk device according to claim 7,

wherein the control mechanism decrypts the read-out data when the data read out of the recording medium are encrypted, and

the control mechanism encrypts and writes the data in the recording medium when the encryption function is turned on.

10. The hard disk device according to claim 7,

wherein the control mechanism includes an encryption function for encrypting desired data and personal identification information by use of an encryption key created out of a given piece of the personal identification information, and

the control mechanism executes user verification by use of the encrypted personal identification information.

11. The hard disk device according to claim 10,

wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and

the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys.

12. The hard disk device according to claim 7,

wherein the control mechanism includes an encryption function for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key created out of a given piece of the personal identification information, and

the control mechanism executes user verification by use of the encrypted personal identification information.

13. An information processing device comprising:

an operation control unit for executing various operation processing; and

a data storage device for storing data to be processed by the operation control unit,

wherein the data storage device includes an encryption function for encrypting desired data by use of a data encryption key and for encrypting personal identification information by use of an verification encryption key created out of a given piece of the personal identification information, and

the data storage device executes user verification by use of the encrypted personal identification information.

14. The information processing device according to claim 13, wherein the data encryption key and the verification encryption are mutually identical.

15. The information processing device according to claim 13, wherein the data storage device encrypts the data encryption key by use of a different encryption key and saves the encrypted data encryption key.

16. The information processing device according to claim 15,

wherein the data storage device encrypts the data encryption key by use of the verification encryption key as the different encryption key.

17. A data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device, the data processing method for a data storage device comprising the steps of:

creating an encryption key out of a given piece of personal identification information;

encrypting the personal identification information by use of the encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data;

executing user verification based on the verification data recorded in the recording medium; and

executing any of encrypting write data transmitted from a host system by use of the encryption key and thereby recording the encrypted write data in the recording medium, and, decrypting the data read out of the recording medium by use of the encryption key and thereby transmitting the decrypted data to the host system.

18. The data processing method for a data storage device according to claim 17, further comprising the steps of:

encrypting the encryption key by use of a different encryption key and thereby recording the encrypted encryption key in the recording medium; and

decrypting the encrypted encryption key by use of the different encryption key and thereby decrypting the data read out of the recording medium by use of the decrypted encryption key.

19. A data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device, the data processing method for a data storage device comprising the steps of:

creating a verification encryption key out of a given piece of personal identification information;

encrypting the personal identification information by use of the verification encryption key and recording the encrypted personal identification information in the recording medium as verification data, and further encrypting a data encryption key by use of the verification encryption key and thereby recording the encrypted data encryption key in the recording medium;

executing user verification based on the verification data recorded in the recording medium;

decrypting the data encryption key recorded in the recording medium by use of the verification encryption key; and

executing any of encrypting write data transmitted from a host system by use of the decrypted data encryption key and thereby recording the encrypted write data in the recording medium, and decrypting the data read out of the recording medium by use of the data encryption key and thereby transmitting the decrypted data to the host system.

20. The data processing method for a data storage device according to claim 19, further comprising the step of:

decrypting the encrypted data encryption key recorded in the recording medium along with a change in the personal identification information by use of the verification encryption key created out of the personal identification information prior to the change, and then encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change and thereby storing the data encryption key in the recording medium.

21. The data processing method for a data storage device according to claim 19, further comprising the step of:

decrypting the encrypted data encryption key recorded in the recording medium upon disabling encryption of the data recorded in the recording medium by use of the verification encryption key created out of the personal identification information prior to a change and thereby storing the decrypted data encryption key in the recording medium.

22. A program for controlling a computer to control data writing and reading in and out of a magnetic disk, the program causing the computer to execute the processes of:

creating an encryption key out of a given piece of personal identification information;

encrypting the personal identification information by use of the encryption key and thereby recording the encrypted personal identification information in the magnetic disk as verification data;

executing user verification based on the verification data recorded in the magnetic disk; and

executing any of encrypting write data transmitted from a host system by use of the encryption key and thereby recording the encrypted write data in the magnetic disk, and decrypting the data read out of the magnetic disk by use of the encryption key and thereby transmitting the decrypted data to the host system.

23. A program for controlling a computer to control data writing and reading in and out of a magnetic disk, the program causing the computer to execute the processes of:

creating an verification encryption key out of a given

piece of personal identification information;

encrypting the personal identification information by use of the verification encryption key and recording the encrypted personal identification information in the magnetic disk as verification data, and further encrypting a data encryption key by use of the verification encryption key and thereby recording the encrypted data encryption key in the magnetic disk;

executing user verification based on the verification data recorded in the magnetic disk;

decrypting the data encryption key recorded in the magnetic disk by use of the verification encryption key; and

executing any of encrypting write data transmitted from a host system by use of the decrypted data encryption key and thereby recording the encrypted write data in the magnetic disk, and decrypting the data read out of the magnetic disk by use of the data encryption key and thereby transmitting the decrypted data to the host system.